WHAT IS CLAIMED IS:

1. A method for strong authentication achieved in a single round trip, comprising:

sending a random number to a mobile node (MN), wherein the random number is generated local to the MN;

generating a MN signature using the MN, wherein the MN signature is generated using the random number;

authenticating the MN to a network, wherein the network is a GPRS network; and

authenticating the network to the MN.

2. The method of Claim 1, wherein authenticating the MN to the network, further comprises sending the MN signature to an authentication server; and verifying, by the authentication server, the mobile node signature.

3. The method of Claim 1, wherein the random number is generated by a base station.

4. The method of Claim 2, wherein authenticating the network to the MN, further comprises generating an authentication signature by the authentication server; and sending the authentication signature to the MN.

5. The method of Claim 4, further comprising: verifying, by the MN, the authentication signature.

6. The method of Claim 5, wherein the authentication server is a home authentication server (AAAH).

7. The method of Claim 6, wherein sending the MN signature to the AAAH, further comprises sending the MN signature to a local authentication server

(AAAF), wherein AAAF is located in a foreign domain and forwards the signature to the AAAH.

8. The method of Claim 7, further comprising determining when the MN signature is not verified, and when ending the strong authentication.

9. The method of Claim 8, further comprising determining when the authentication signature is not verified, and when ending the strong authentication.

10. A system for strong authentication achieved in a single round trip between a MN and a network, comprising:

a mobile node (MN) that is configured to generate a MN signature in response to a random number received from a source within a domain local to a current position relating to the MN and send the MN signature to be verified;

the authentication server located within a home domain associated with the MN that is configured to receive the MN signature, verify the MN signature, and in response to the verification of the MN signature that indicates that the MN is verified to the network, wherein the network is a GPRS network, return an authentication signature to the MN.

11. The system of Claim 10, wherein the source comprises a base station, wherein the base station is within the domain local to the MN and is configured to generate the random number and send the random number to the MN.

12. The system of Claim 10, further comprising: the MN is configured to verify the authentication signature, and if the authentication signature is verified authenticating the network to the MN.

13. The system of Claim 11, further comprising: the MN is configured to verify the authentication signature, and if the authentication signature is verified authenticating the network to the MN.

14. The system of Claim 13, wherein the authentication server is a home authentication server (AAAH).

15. The system of Claim 14, wherein sending the MN signature to be verified, further comprises the MN is configured to send the MN signature to a local authentication server (AAAF), and the AAAF is configured to forward the signature to the AAAH.

16. The system of Claim 15, wherein the AAAH is further configured to send the authentication signature to the AAAF, wherein the AAAF is arranged to send the authentication signature to the MN.

17. The system of Claim 16, wherein the AAAH is further configured to determine when the MN signature is not verified, and when, end the strong authentication.

18. The system of Claim 17, wherein the MN is further configured to determine when the authentication signature is not verified, and when, end the strong authentication.

19. A system for strong authentication between a mobile node (MN) and a network, comprising:

a means for generating a random number local to the MN;

a means for sending the random number to the mobile node

a means for generating a MN signature using the MN, wherein the MN signature is generated using the random number;

a means for sending the MN signature to an authentication server within a GPRS network, and verifying by the authentication the MN signature; and in response to the verifying, generating an authentication signature and sending the authentication signature to the MN for verification.